

(11)Publication number : 11-328032
(43)Date of publication of application : 30.11.1999

G06F 12/14

(71)Applicant : NEC CORP
(72)Inventor : MORISHITA TAKUYA

Copyright (C); 1998,2000 Japanese Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-328032

(43)公開日 平成11年(1999)11月30日

(51)Int.Cl.⁹

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

3 2 0 A

3 2 0 B

審査請求 有 請求項の数 5 O L (全 7 頁)

(21)出願番号 特願平10-125619

(22)出願日 平成10年(1998)5月8日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 森下 卓也

東京都港区芝5丁目7番1号 日本電気株式会社内

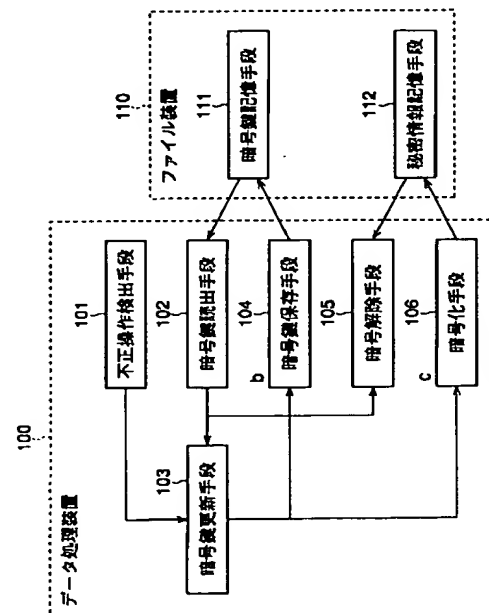
(74)代理人 弁理士 小橋川 洋二

(54)【発明の名称】 ソフトウェアの不正利用防止システム

(57)【要約】

【課題】 いかなるモードで動作するソフトウェアデバッガを用いても解析不能であり、秘密情報を別装置にバックアップしても該秘密情報の読み取りを不可能にしたソフトウェアの不正利用防止システムを提供する。

【解決手段】 秘密情報を記憶する秘密情報記憶手段112と、該秘密情報記憶手段に記憶した秘密情報を解く暗号鍵を記憶する暗号鍵記憶手段110と、当該システムに対するアクセスの正否を判断するアクセス正否判断手段(不正操作検出手段)101と、該アクセス正否判断手段の判断が正の場合には秘密情報記憶手段に記憶させる秘密情報の再暗号化鍵と暗号鍵記憶手段に記憶させる再暗号化鍵とを同一にしてアクセス毎に更新し、前記判断が否の場合には前記2種の再暗号化鍵を異なった鍵としてアクセス毎に更新する暗号鍵更新手段とを備えた。



【特許請求の範囲】

【請求項1】 秘密情報を記憶する秘密情報記憶手段と、

該秘密情報記憶手段に記憶した秘密情報を解く暗号鍵を記憶する暗号鍵記憶手段と、

当該システムに対するアクセスの正否を判断するアクセス正否判断手段と、

該アクセス正否判断手段の判断が正の場合には前記秘密情報記憶手段に記憶させる秘密情報の再暗号化鍵と前記暗号鍵記憶手段に記憶させる再暗号化鍵とを同一にしてアクセス毎に更新し、前記判断が否の場合には前記2種の再暗号化鍵を異なった鍵としてアクセス毎に更新する暗号鍵更新手段とを備えたことを特徴とするソフトウェアの不正利用防止システム。

【請求項2】 秘密情報を記憶する秘密情報記憶手段と、該秘密情報記憶手段に記憶した秘密情報を解く暗号鍵を記憶する暗号鍵記憶手段とを備えたソフトウェアの不正利用防止システムにおいて、

当該システムに対するアクセスの正否を判断する工程と、

該アクセス正否判断の工程で、判断が正の場合には前記秘密情報記憶手段に記憶させる秘密情報の再暗号化鍵と前記暗号鍵記憶手段に記憶させる再暗号化鍵とを同一にしてアクセス毎に更新し、前記判断が否の場合には前記2種の再暗号化鍵を異なった鍵としてアクセス毎に更新する工程とを備えたことを特徴とするソフトウェアの不正利用防止システム。

【請求項3】 秘密情報を記憶する秘密情報記憶手段と、該秘密情報記憶手段に記憶した秘密情報を解く暗号鍵を記憶する暗号鍵記憶手段とを備えたソフトウェアの不正利用防止システムにおいて、

当該システムに対するアクセスの正否を判断する処理と、

該アクセス正否判断の処理で、判断が正の場合には前記秘密情報記憶手段に記憶させる秘密情報の再暗号化鍵と前記暗号鍵記憶手段に記憶させる再暗号化鍵とを同一にしてアクセス毎に更新処理し、前記判断が否の場合には前記2種の再暗号化鍵を異なった鍵としてアクセス毎に更新する処理とをコンピュータに実行させるためのプログラムを記憶した記録媒体。

【請求項4】 前記秘密情報記憶手段と前記暗号鍵記憶手段とは、別個に構成した記憶手段であることを特徴とする請求項1乃至請求項3のいずれかに記載のソフトウェアの不正利用防止システム。

【請求項5】 前記請求項1乃至請求項4のいずれかに記載の発明を、ICカードに適用したことを特徴とするソフトウェアの不正利用防止システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ソフトウェアの不正

正利用防止システムに関し、特にICカード等を一般ユーザに配付した場合に、不正利用者によりICカード等に格納した秘密情報が解読されないようにしたソフトウェアの不正利用防止システムにする。

【0002】

【従来の技術】 例えば医療用のICカードには患者に関する秘密情報がソフトウェアとして格納されているので、第三者によりその秘密情報が解読され不正利用されるのを防止する必要がある。従来、ソフトウェアの不正利用防止システムとして、例えば次の2つの手段が知られている。

【0003】 第1の手段は図5に示すもので、具体的にはマイクロコンピュータ（半導体集積回路装置）のオペレーティングシステム（OS）を構成する制御プログラムの秘匿の技術に関するものである（特開平8-185361号公報）。図5において、マイクロコンピュータ1には、OSのカーネル等の制御プログラムが格納される書き換え可能な不揮発性メモリのシステムメモリ（記憶手段）2が設けられている。該システムメモリ2には、暗号化された制御プログラム等のデータを復号化する所定の復号アルゴリズムに基づく復号鍵FKと、該復号鍵FKを用いて復号アルゴリズムを処理するプログラムからなる復号手続きFTが格納されている。前記復号鍵FKおよび復号手続きFTは、システムメモリ2に格納されるので、ユーザは書き換えを任意に行うことができる。前記暗号化の方式としては、暗号化および復号化を同一の鍵で行う対称暗号系方式と、暗号化の鍵と復号化の鍵が異なる非対称暗号系方式とがあり、どちらの方式にも適用できる。暗号化ならびに復号化は、所定のビット列における交換または反転等の可逆的操作を鍵を用いて制御する。

【0004】 マイクロコンピュータ1には、外部バスBgを介してデータの入出力を行う入出力回路3と、該入出力回路3から入力された所定のデータを格納するRAM4が設けられている。マイクロコンピュータ1には、該マイクロコンピュータ1の全ての制御を司るCPU（中央処理装置）5が設けられ、CPU5と復号鍵FKと復号手続きFTとで復号化手段FSが構成される。前記システムメモリ2、入出力回路3、RAM4、CPU5は、内部バス6を介して接続されている。

【0005】 このような構成を有する従来のソフトウェア不正利用防止システムは、次のような手段で秘密情報を不正利用者から保護している。即ち、CPU5が有する命令・データに対する保護機能を使用しているのである。前記システムメモリ2はスーパーバイザモード以外からのアクセスが禁止されている。このため、システムメモリ2に格納される秘密情報を通常のユーザが取り出すことは一般的にはできない。

【0006】 また、第2の不正利用防止手段としては、秘密情報を格納した専用装置を使用した構成では、不正

利用者による物理的な分析が行われた場合には、物理的に前記専用装置を破壊する措置を講じることである。

【0007】

【発明が解決しようとする課題】しかしながら、前記の第1、第2のソフトウェアの不正利用防止手段には、それぞれ次のような問題点があった。

【0008】第1の不正利用防止手段に対する問題点は、ソフトウェアによる秘密情報の保護が完全ではない（不十分である）という点である。その理由は、第1の手段における秘密情報保護手段が、スーパーバイザモード以外でアクセスするのを禁止しているだけであり、若し不正利用者がスーパーバイザモードで動作するソフトウェアデバッガで解析を行った場合には、秘密情報の保護は無効化されてしまうからである。

【0009】第2の不正利用防止手段に対する問題点は、ソフトウェアのみの構成の場合には、自己破壊して不正利用を防止する機構が備わっていないという点である。その理由は、ソフトウェアのみの構成の場合、秘密情報自体を一般的なファイル装置に格納せざるを得ず、そのため秘密情報を他のファイル装置にバックアップすることが可能である。従って、秘密情報を破壊したとしても、不正利用者が予め別のファイル装置に秘密情報をバックアップしておけばそれをリストアするのは容易だからである。

【0010】そこで本発明の課題は、いかなるモードで動作するソフトウェアデバッガを用いても解析不能であり、秘密情報を別装置にバックアップしても該秘密情報の読み取りを不可能にしたソフトウェアの不正利用防止システムを提供することである。

【0011】

【課題を解決するための手段】前記課題を解決するために本発明は、秘密情報を記憶する秘密情報記憶手段と、該秘密情報記憶手段に記憶した秘密情報を解く暗号鍵を記憶する暗号鍵記憶手段と、当該システムに対するアクセスの正否を判断するアクセス正否判断手段と、該アクセス正否判断手段の判断が正の場合には前記秘密情報記憶手段に記憶させる秘密情報の再暗号化鍵と前記暗号鍵記憶手段に記憶させる再暗号化鍵とを同一にしてアクセス毎に更新し、前記判断が否の場合には前記2種の再暗号化鍵を異なった鍵としてアクセス毎に更新する暗号鍵更新手段とを備えたことを特徴とする。

【0012】このようにすれば、不正利用者がアクセスして秘密情報記憶手段内にある秘密情報の暗号化を解除しようとしても解除することができず、また正常利用者がアクセスして正常処理をすれば秘密情報記憶手段内の秘密情報の暗号化を解除することができる。従って、不正利用者がソフトウェア内に含まれる秘密情報を得ようとする試みの防止を可能にすることができる。

【0013】

【発明の実施の形態】以下、本発明を図示の実施形態例

に基づいて説明する。

【0014】〔1〕実施形態例の構成

【0015】図1は、本実施形態例のソフトウェアの不正利用防止システムの構成を示すブロック図である。図1に示すように、本実施形態例のソフトウェアの不正利用防止システムは、プログラム制御により動作するデータ処理装置100と、ファイル装置（記憶装置）110とを備えている。

【0016】データ処理装置100は、次にそれぞれ説明する「アクセス正否判断手段」である不正操作検出手段101と、暗号鍵読出手段102と、暗号鍵更新手段103と、暗号鍵保存手段104と、暗号解除手段105と、暗号化手段106を含む。ファイル装置110は、暗号化された秘密情報が格納された秘密情報記憶手段112と、該秘密情報記憶手段112に格納された秘密情報を暗号化解除するのに必要な暗号鍵が格納された暗号鍵記憶手段111とを含む。前記暗号鍵記憶手段111と秘密情報記憶手段112とは、1回のバックアップ等の操作で同時に復元されるのを防ぐため、同一のファイル装置内には格納せず、別個のファイル装置に格納する。即ち、2回のバックアップ操作を行わなければ、暗号鍵と秘密情報とをバックアップできないようにしておく。

【0017】前記各手段101～106は、それぞれ次の動作を行う。不正操作検出手段101は、秘密情報（秘密鍵暗号方式の秘密鍵や暗号アルゴリズムそのもの等）を得ようとする不正利用者が、秘密情報の暴露を試みているか否かを検出し（検出手段は次に説明する）、暴露の試みが行われていた場合には次に説明する暗号鍵更新手段103に通知を行う。暗号鍵読出手段102は、暗号鍵記憶手段111より秘密情報を暗号化解除するための暗号鍵aを読み出す。

【0018】暗号鍵更新手段103は、次に説明するように区分けして暗号鍵を更新し、暗号鍵保存手段104と暗号化手段106に更新した新しい暗号鍵を送る。この時、不正操作検出手段101によって秘密情報の暴露の試みが検出されていた場合には、暗号鍵更新手段103は、暗号鍵保存手段104に対して送信する暗号鍵bと暗号化手段106に送信する暗号鍵cを全く異なったものとする（暗号鍵b≠暗号鍵c）。また、暗号鍵更新手段103は、正常な動作時（秘密情報の暴露の試みがされていない場合）には、暗号化手段106と暗号鍵保存手段104に送信する新しい暗号鍵bならびに暗号鍵cを同一のものとする（暗号鍵b＝暗号鍵c）。

【0019】暗号鍵保存手段104は、暗号鍵更新手段103が更新した新しい暗号鍵bを暗号鍵記憶手段111に保存する。暗号解除手段105は、秘密情報記憶手段112から暗号化された秘密情報を読み出し、暗号鍵読出手段102が読み出した暗号鍵aで暗号化解除を行い、本来の処理に必要な秘密情報を得る。暗号化手段1

06は、暗号解除手段105が暗号化解除した秘密情報を暗号鍵更新手段103が更新した新しい暗号鍵cで再暗号化し、秘密情報記憶手段112に保存する。

【0020】[II]動作説明

次に本実施形態例の動作を、前記図1と、図2に示すフローチャートを参照しつつ詳細に説明する。

【0021】まず、暗号鍵読出手段102は、暗号鍵記憶手段111より暗号鍵aを読み出す(図2のステップA1)。次に、不正操作検出手段101は、秘密情報を得ようとする不正利用者が秘密情報の暴露を試みているか否かを検出する(ステップA2)。この検出は、例えばデータ処理装置100上で動作しているこのソフトウェア不正利用防止システム自体を不正利用者が改竄していないかを検査する。この検査は、秘密鍵暗号を利用した電子署名による改竄検出等で行う。また、ソフトウェアデバッグによるプログラム動作の解析も同時に検出する。

【0022】暗号鍵更新手段103は、秘密情報を再暗号化する暗号鍵の更新を行う(ステップA3またはステップA4)。即ち、ステップA2で不正操作検出手段101によって不正操作が検出されていない場合には(ステップS2: no)、暗号鍵更新手段103は、暗号鍵保存手段104が暗号鍵記憶手段111に保存する暗号鍵bと暗号化手段106が秘密情報の再暗号化に使用する暗号鍵cとを同一のものとする(暗号鍵b=暗号鍵c)(ステップA3)。また、前記不正操作が検出されている場合には(ステップS2: yes)、暗号鍵更新手段103は、暗号鍵bと暗号鍵cを全く異なるものとする(暗号鍵b≠暗号鍵c)(ステップA4)。ここに、暗号鍵更新手段103が行う新しい暗号鍵の生成は、一方向関数や疑似乱数等を使用して、暗号鍵bから暗号鍵aおよび暗号鍵cを容易に算出できないような処理とする。

【0023】暗号解除手段105は、秘密情報記憶手段112から暗号化された秘密情報を読み出し、暗号鍵読出手段102が読み出した暗号鍵aで暗号化解除を行い暗号化されていない秘密情報を展開し(ステップA5)、この秘密情報を使用した処理、例えば秘密鍵暗号を使用した商取引の認証処理等を行う(ステップA6)。暗号化手段106は、暗号化解除手段105が暗号化解除した秘密情報を暗号鍵更新手段103が更新した暗号鍵cで再暗号化し(ステップA7)、再暗号化した秘密情報を秘密情報記憶手段112に保存する(ステップA8)。暗号鍵保存手段104は、暗号鍵更新手段103が更新した暗号鍵bを暗号鍵記憶手段111に保存する(ステップA9)。

【0024】[III]具体例による説明

次に、具体例について、図3および図4を用いて説明する。

【0025】(1)不正操作の試み無しの場合

図3は、不正利用者による不正操作の試みが行われなかった場合の動作を表す説明図である。

【0026】図3に示すように、例えば、暗号鍵記憶手段111には最初、暗号鍵a1(値は01010101)が格納され、秘密情報記憶手段112には暗号鍵a1で暗号化された秘密情報が格納されている。なお、ここでは説明の簡略化のために、暗号鍵の鍵長は8ビットとしたが、実際は暗号化アルゴリズムの強度に応じてもっと長い(一般的には数十～数千ビット)鍵を使用する。一回目のアクセス実行時のステップA1で暗号鍵読出手段102は、暗号鍵記憶手段111から暗号鍵a1を読み出す。前述の如くこの場合はステップA2で不正操作が検出されなかったため、ステップA3で更新される2つの新しい暗号鍵b1と暗号鍵c1とは同じ値(10111000)となる(暗号鍵b1=暗号鍵c1)。暗号解除手段105は、最初の暗号鍵a1を用いて秘密情報を暗号化解除する(ステップA5)。暗号化手段106は、新しい暗号鍵c1(10111000)を用いて暗号化解除された秘密情報を再暗号化する(ステップA7)。また、暗号鍵保存手段104は、新しい暗号鍵b1(10111000)を暗号鍵記憶手段111に保存する(ステップA9)。

【0027】二回目のアクセス実行時のステップA1で暗号鍵読出手段102は、前記ステップS9で暗号鍵記憶手段111に保存された暗号鍵b1(=暗号鍵a2)(10111000)を読み出す。暗号解除手段105は、この暗号鍵a2で暗号鍵記憶手段111に格納されている秘密情報の暗号化を解除する(ステップA5)。秘密情報は、一回目の実行時に暗号鍵c1(=暗号鍵b1)(10111000)を用いて暗号化されている。この時、暗号鍵a2と暗号鍵c1は同じ値(10111000)のため暗号解除は正しく行われ、正しい秘密情報を得ることが可能である。三回目以降も同様の処理が行われ、毎回秘密情報を暗号化する暗号鍵は更新されるが、正しい秘密情報を得ることができる。

【0028】(2)不正操作の試み有りの場合

図4は不正利用者による不正操作の試みが行われた場合の動作を表す説明図である。

【0029】図4に示すように、例えば、暗号鍵記憶手段111には最初、暗号鍵a1(値は01010101)が格納され、暗号鍵記憶手段111には暗号鍵a1で暗号化された秘密情報が格納されている。一回目の実行時のステップA1で、暗号鍵読出手段102は暗号鍵a1を読み出す。ステップA2で不正操作が検出されたため、ステップA3で更新される2つの新しい暗号鍵b1と暗号鍵c1は異なる値(10111000と11100101)となる(暗号鍵b1≠暗号鍵c1)。

【0030】暗号解除手段105は、暗号鍵a1を用いて秘密情報を暗号化解除する(ステップA5)。暗号化手段106は、新しい暗号鍵c1(11100101)

10

20

30

40

50

を用いて暗号化解除された秘密情報を再暗号化する（ステップA7）。また、暗号鍵保存手段104は新しい暗号鍵b1（10111000）を暗号鍵記憶手段111に保存する（ステップA9）。二回目の実行時のステップA1で、暗号鍵読出手段102は暗号鍵a2（10111000）を読み出す。暗号解除手段105は、この暗号鍵a2で暗号鍵記憶手段111に格納されている秘密情報の暗号化を解除する（ステップA5）。秘密情報は、一回目の実行時に暗号鍵c1（11100101）を用いて暗号化されている。この時、暗号鍵a2と暗号鍵c1は異なる値（10111000と11100101）のため暗号解除は正常に行われず、正しい秘密情報とはならない。

【0031】この状態になってから不正利用者が正しい秘密情報を得るためには、暗号鍵c1の値（11100101）を何らかの方法で知る必要がある。この値はファイル装置110の中に保存されていないため、暗号鍵を総当たりで試す必要がある。この場合は、暗号化アルゴリズムや鍵長に依存するが、実用上十分な強度を得ることは可能である。また、一回目の実行前に予め暗号鍵記憶手段111に格納されている暗号鍵a1（01010101）で暗号化された秘密情報を他のファイル装置にバックアップしておいて、この状態（前述の正しい秘密情報とならない状態）になったらその暗号化された秘密情報をリストアするという手法も考えられるが、やはり暗号鍵a1の値は失われているため秘密情報を復元するのは困難である。

【0032】更に一回目の実行前に暗号鍵記憶手段111に格納されている暗号鍵a1の値も同時に別のファイル装置にバックアップしておけば秘密情報の復元は不可能ではないが、こういった構造を正確に知るためには実際にソフトウェアデバッグによる解析（即ち、不正操作検出手段101が検出する不正操作）を行わない限り困難である。三回目以降も同様の処理が行われ、正しい秘密情報は得られなくなる。この処理を繰り返すと、毎回異なった暗号鍵で暗号化と暗号化解除が行われるため、秘密情報の復元は更に困難となる。

【0033】なお、本発明は多数の一般人に配付されることが多いICカードに適用するのに好適であるが、そ

の他に例えば電子商取引に使用する第三者に知られてはならない秘密情報（認証用の秘密鍵）を持ったソフトウェアやマイクロコンピュータ（半導体集積回路装置）等を配布する際にも適用することが可能である。

【0034】

【発明の効果】以上説明したように本発明によれば、アクセス正否判断手段（不正操作検出手段）を設け、不正を検出した場合には、2回目以降の動作時に秘密情報の暗号化解除をできなくなるようにしているので、ソフトウェアデバッグでの解析およびソフトウェアを改竄して不正に秘密情報を得ることを防止することができる。また、暗号鍵記憶手段と秘密情報記憶手段を別のファイル装置にバックアップし、不正操作を検出した際に暗号鍵を別々のものにしているので、不正操作の結果正常に動作しなくなってからバックアップした秘密情報をリストアしたとしても、正常な動作を不可能にすることができる。

【図面の簡単な説明】

【図1】本発明の実施形態例のブロック図である。

20 【図2】同実施形態例の動作を示すフローチャートである。

【図3】同実施形態例における正常アクセス時の動作を説明する説明図である。

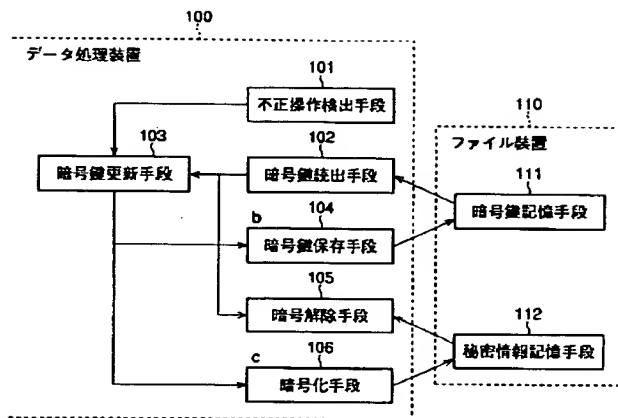
【図4】同実施形態例における否正常アクセス時の動作を説明する説明図である。

【図5】従来のソフトウェアの不正利用防止システムの一例のブロック図である。

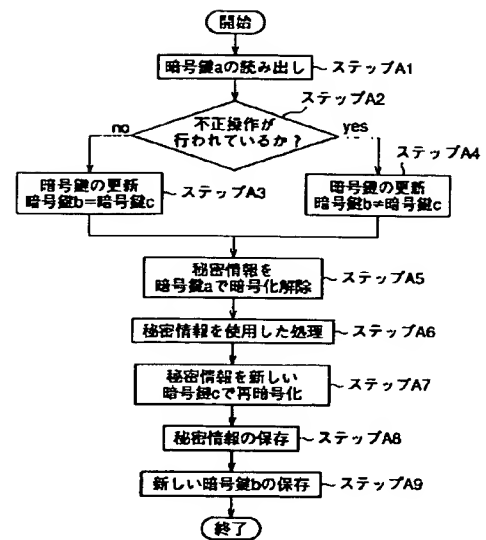
【符号の説明】

- 100 データ処理装置
- 30 101 不正操作検出手段（アクセス正否判断手段）
- 102 暗号鍵読出手段
- 103 暗号鍵更新手段
- 104 暗号鍵保存手段
- 105 暗号解除手段
- 106 暗号化手段
- 110 ファイル装置
- 111 暗号鍵記憶手段
- 112 秘密情報記憶手段

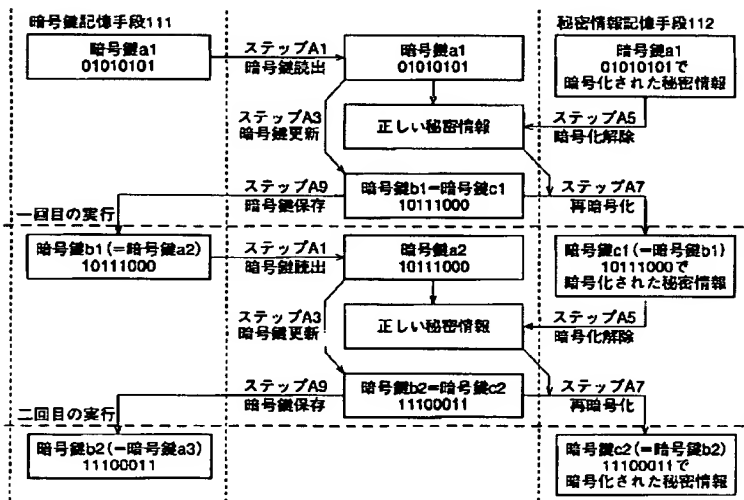
【図1】



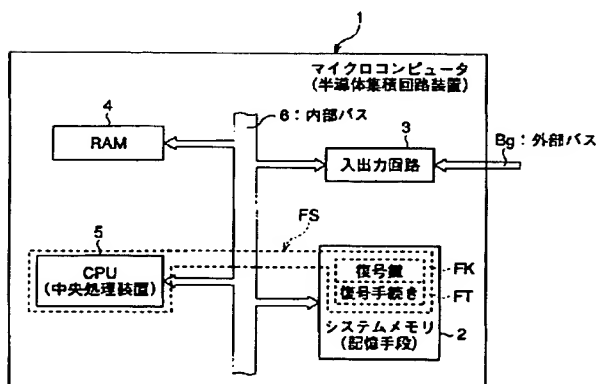
【図2】



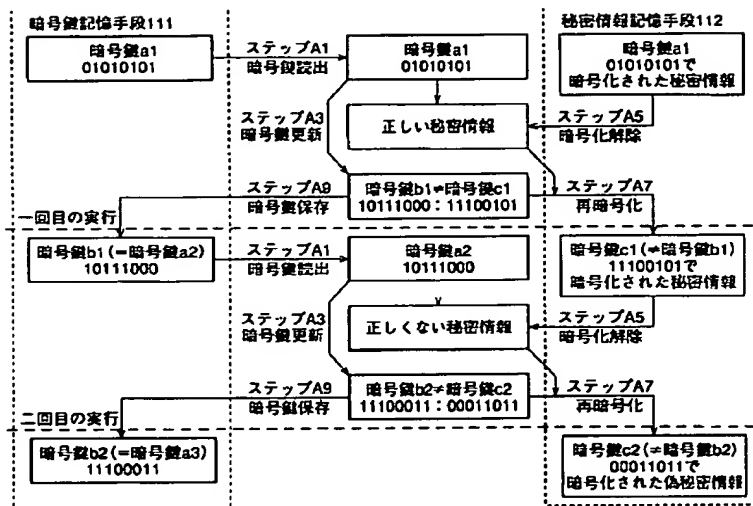
【図3】



【図5】



【図4】



THIS PAGE BLANK (USPTO)